SINGLE SIGN-ON FRAMEWORK WITH TRUST-LEVEL MAPPING TO AUTHENTICATION REQUIREMENTS

David L. Wood,
Derk Norton,
Paul Weschler,
Chris Ferris and
Yvonne Wilson

ABSTRACT OF THE DISCLOSURE

A security architecture has been developed in which a single sign-on is provided for multiple information resources. Rather than specifying a single authentication scheme for all information resources, the security architecture associates trust-level requirements with information resources. Authentication schemes (e.g., those based on passwords, certificates, biometric techniques, smart cards, etc.) are associated with trust levels and a log-on service obtains credentials for an entity commensurate with the trust-level requirement(s) of an information resource (or information resources) to be accessed. Once credentials have been obtained for an entity and the entity has been authenticated to a given trust level, access is granted, without the need for further credentials and authentication, to information resources for which the authenticated trust level is sufficient.